WHAT CAN YOU DO *TODAY* TO PROTECT DATA?

Here are some specific BioSci recommendations:

1. **Know your data and where it is stored** – maintain an up-to-date inventory (e.g., laptops, PCs, servers, software, media (USB, CD-ROM, DVD), hosted cloud storage). **If you have sensitive research data,** please contact us. We maintain an inventory with OIT to ensure that any research data with PII or other restricted data is properly accounted for.
2. **Back up data regularly and test periodically** – online and offline. Backups need to be physically separate (on a different system) from the primary copy of data. A standard external drive (available at any vendor) works well with drag and drop. There are also UC-sanctioned cloud services such as Google Drive and Microsoft OneDrive that allow you to drag and drop files for safe keeping as well as collaborate with your researchers. Please contact us with any questions.
3. **Use strong passwords** of at least 12 characters or more and multi-factor authentication (e.g., DUO). We recommend using a password manager such as LastPass or 1Password to maintain multiple passwords. The campus has licensed LastPass for all campus employees. Click here for more information.
4. **Ensure anti-malware software is installed**, running and up to date. We recommend using Windows 10's built-in Windows Defender software. For Macs, we recommend Sophos Anti-Virus. Please contact us for installation information.

When in doubt, please ask! We are happy to answer your questions on research security concerns. You may also want to check the campus security website at security.uci.edu.

Adapted from Vice Chancellor for Research Pramod Khargonekar's message, "UC Irvine Response to Research Data Ransomware Threat" on 8/25/20